

Asset-Based Reporting for CyberScope



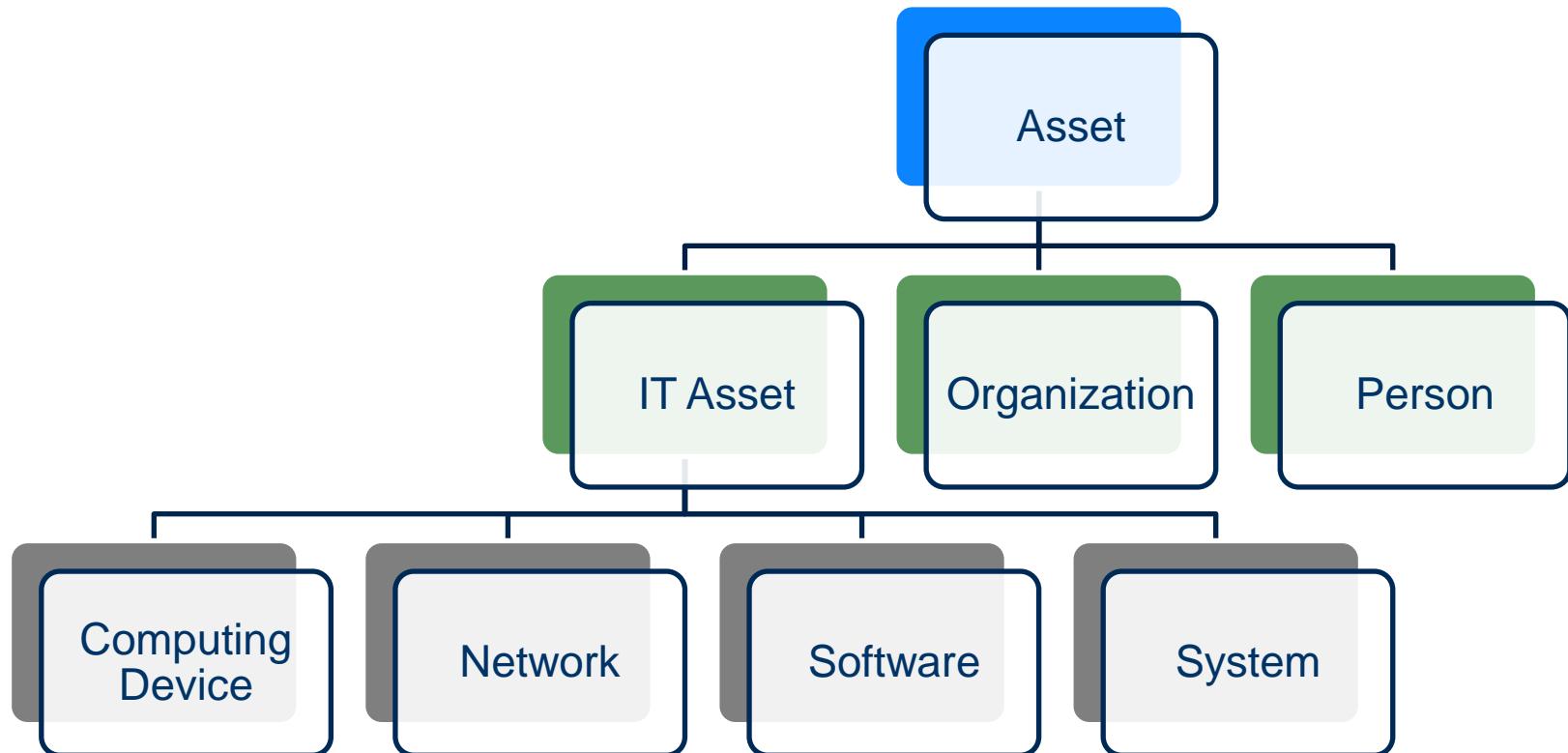
Agenda

- Discuss Overall Objectives
- Review the Asset Identification Model
- Review the Asset Reporting Format (ARF) 1.0 Model
- Review the Lightweight Asset Reporting Format (LASR)
- Discuss vendor collaboration opportunities
- Questions and Feedback

Overall Objectives

- Provide a standardized enterprise reporting format that will support government wide situational awareness regarding:
 - Vulnerability Management
 - Configuration Management Baselines
 - Software Inventory
- Enable scalable, automated reporting on a short-term, periodic basis
- Leverage current efforts within the security automation community
- Minimize vendor development costs, while maximizing product interoperability

The Asset Identification Model



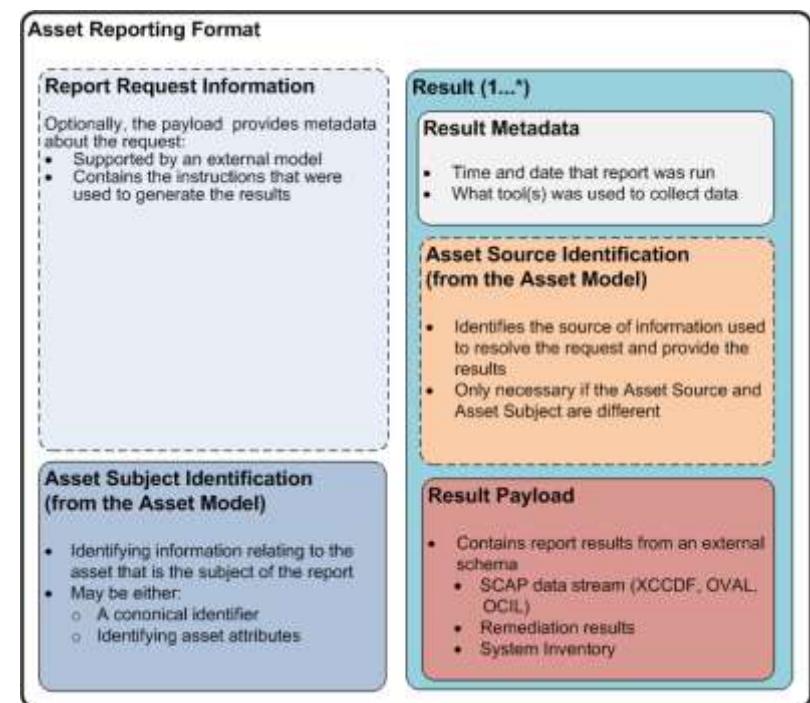
The Asset Identification Model

- Provides common asset types to support management, reporting, and correlation use cases
- Enables asset identification by:
 - Canonical identifier
 - Organizationally unique identifier
 - Manufacturer identifier
 - etc.
 - One or more asset properties
 - Name
 - Network Information
 - Common Platform Enumeration (CPE) Name
 - etc.

The Asset Reporting Format (ARF) 1.0 Model

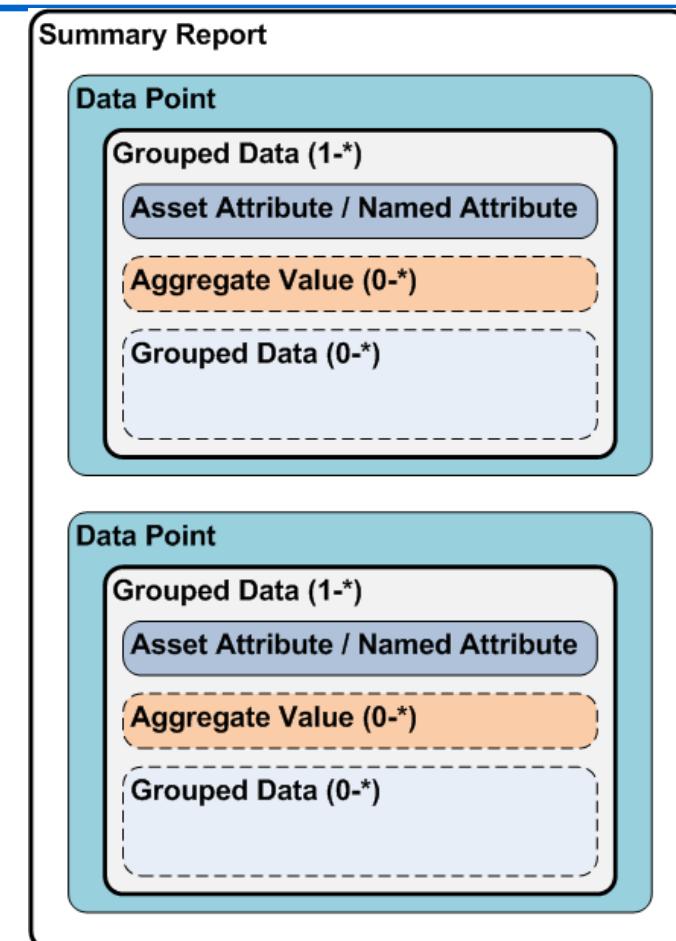
The Asset Reporting Format contains:

- Information about the request
- The subject of the report
- The report result(s)
 - The source of the report data
 - The report payload



The Lightweight Asset Summary Reporting (LASR) Model

- Modeled after SQL GROUP BY semantics
- A hierarchically organized collection of *attributes*, *aggregate values*, and groupings
- Each *Data Point* represents an individual reporting element
- *Grouped Data* enables reporting multiple collections of *attributes* and *aggregate values* for the same context
- *Attributes* represent the named properties of the aggregate data
- *Aggregate values* represent counts, sums and averages



The FISMA Reporting Auto-Feeds

- Machine-readable, XML-based format
- Uses ARF, Asset Identification and LASR to support automated report generation
- Uses SCAP enumerations (CVE, CCE, and CPE) and other concepts as part of the standardized reporting vocabulary
- Reports must be producible by automated tools

Example – ARF Data

```
<?xml version="1.0" encoding="UTF-8"?>
<AssetReport ...>
  <Subject>
    <ai:Organization>
      <xNL:OrganisationNameDetails>
        <xNL:OrganisationName>Department of Commerce</xNL:OrganisationName>
        <xNL:OrganisationName>National Institute of Standards and Technology</xNL:OrganisationName>
        <xNL:OrganisationName>Information Technology Laboratory</xNL:OrganisationName>
        <xNL:OrganisationName>Computer Security Division</xNL:OrganisationName>
      </xNL:OrganisationNameDetails>
    </ai:Organization>
  </Subject>
  <ReportInformation>
    <Report>
      <ReportMetadata>
        <DateTime>2006-05-04T18:13:51.0Z</DateTime>
        <Tool>
          <ai:Software>
            <ai:CPE>cpe:/a:vendor_a:reporting_manager:1.2.3.45</ai:CPE>
          </ai:Software>
        </Tool>
      </ReportMetadata>
      <ReportPayloads>
        <ReportPayload>
          <sr:SummaryReport id="FISMA_auto_feed_fy10" version="1.0beta1">
            ...
            </sr:SummaryReport>
          </ReportPayload>
        </ReportPayloads>
      </Report>
    </ReportInformation>
  </AssetReport>
```

The reporting organization

The report timestamp

The tool that generated the report

The report body

Example – LASR – Configuration Baseline Compliance

Associates specific SCAP checklists and profiles with the aggregate count of compliant systems and exceptions on a per CCE identifier basis

```
<sr:SummaryReport id="FISMA_auto_feed_fy10" version="1.0beta1">
  <sr:DataPoint id="configuration_management_agency_deviations">
    <sr:GroupedData>
      <sr:NamedAttribute name="checklist_name">USGCB-Windows-7</sr:NamedAttribute>
      <sr:GroupedData>
        <sr:NamedAttribute name="checklist_version">v0.1.0.6</sr:NamedAttribute>
        <sr:GroupedData>
          <sr:NamedAttribute name="checklist_profile">united_states_government_configuration_baseline_1.0.1.0</sr:NamedAttribute>
          <sr:AggregateValue name="number_of_systems" type="COUNT">100</sr:AggregateValue>
          <sr:GroupedData>
            <sr:NamedAttribute name="http://cce.mitre.org">CCE-9289-0</sr:NamedAttribute>
            <sr:AggregateValue name="non_compliant_systems" type="COUNT">90</sr:AggregateValue>
            <sr:AggregateValue name="number_of_exceptions" type="COUNT">5</sr:AggregateValue>
          </sr:GroupedData>
        </sr:GroupedData>
        <sr:GroupedData>
          <sr:NamedAttribute name="checklist_profile">agency_profile</sr:NamedAttribute>
          <sr:AggregateValue name="number_of_systems" type="COUNT">100</sr:AggregateValue>
          <sr:GroupedData>
            <sr:NamedAttribute name="http://cce.mitre.org">CCE-9289-0</sr:NamedAttribute>
            <sr:AggregateValue name="non_compliant_systems" type="COUNT">90</sr:AggregateValue>
            <sr:AggregateValue name="number_of_exceptions" type="COUNT">5</sr:AggregateValue>
          </sr:GroupedData>
        </sr:GroupedData>
      </sr:GroupedData>
    </sr:DataPoint>
  </sr:SummaryReport>
```

Example – LASR – Vulnerabilities

Associates each CVE identifier with the number of hosts affected

```
<sr:SummaryReport id="FISMA_auto_feed_fy10" version="1.0beta1">
  <sr:DataPoint id="vulnerability_management_system_vulnerabilities">
    <sr:GroupedData>
      <sr:NamedAttribute name="http://cve.mitre.org/">CVE-2010-1234</sr:NamedAttribute>
      <sr:AggregateValue name="number_of_affected_systems">90</sr:AggregateValue>
    </sr:GroupedData>
    <sr:GroupedData>
      <sr:NamedAttribute name="http://cve.mitre.org/">CVE-2010-5678</sr:NamedAttribute>
      <sr:AggregateValue name="number_of_affected_systems">90</sr:AggregateValue>
    </sr:GroupedData>
  </sr:DataPoint>
</sr:SummaryReport>
```

Example – LASR – OS Inventory

Associates CPE Names with the number of installed hosts

```
<sr:SummaryReport id="FISMA_auto_feed_fy10" version="1.0beta1">
  <sr:DataPoint id="inventory_management_product_inventory">
    <sr:GroupedData>
      <sr:AssetAttribute>
        <ai:Software>
          <ai:CPE>cpe:/o:microsoft:windows_xp::sp2</ai:CPE>
        </ai:Software>
      </sr:AssetAttribute>
      <sr:AggregateValue name="number_of_systems" type="COUNT">100</sr:AggregateValue>
    </sr:GroupedData>
  </sr:DataPoint>
</sr:SummaryReport>
```

Next Steps / Community Participation

- Post schema to SCAP website:
<http://scap.nist.gov/use-case/cyberscope/>
- Specification public comment releases:
 - NIST IR 7693: *The Specification for Asset Identification Version 1.0 (DRAFT)* – 9/2010
 - NIST IR 7694: The Specification for the Asset Reporting Format (ARF) 1.0 (DRAFT) – 9/2010
- Community engagement and feedback
 - NIST Emerging Specifications List
emerging-specs@nist.gov
 - NIST IT Security Automation Conference
September 27-29, Baltimore, MD
Baltimore Convention Center

Questions & Answers / Feedback



David Waltermire

SCAP Architect

Computer Security Division

Information Technology Laboratory
National Institute of Standards and
Technology

david.waltermire@nist.gov

(301) 975-3390